HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

BÁO CÁO BÀI THỰC HÀNH
HỌC PHẦN: THỰC TẬP CƠ SỞ
MÃ HỌC PHẦN: INT13147

BÀI THỰC HÀNH 2.1
CÀI ĐẶT, CẤU HÌNH MẠNG DOANH NGHIỆP VỚI PFSENSE FIREWALL

Sinh viên thực hiện:

B22DCAT253 Đinh Thị Thanh Tâm

Giảng viên hướng dẫn: TS. Đinh Trường Duy

HỌC KỲ 2 NĂM HỌC 2024-2025

MỤC LỤC

CHƯƠNG 1. LÝ THUYẾT BÀI THỰC HÀNH

1.1 Mục đích

- Các công ty thường bảo vệ hệ thống mạng bằng cách sử dụng tường lửa phần cứng hoặc phần mềm để kiểm soát lưu lượng mạng truy cập. Một số loại lưu lượng nhất định có thể bị chặn hoặc cho phép đi qua tường lửa. Việc hiểu cách thức hoạt động của tường lửa và mối quan hệ của nó với các mạng bên trong và bên ngoài sẽ rất quan trọng để có hiểu biết về bảo mật mạng.
- Bài thực hành này giúp sinh viên có thể tự cài đặt, xây dựng một mạng doanh nghiệp với tường lửa để kiểm soát truy cập. Mạng mô phỏng môi trường mạng doanh nghiệp này có thể sử dụng trong các bài lab về ATTT sau này.

1.2 Tìm hiểu về cấu hình mạng trong phần mềm mô phỏng Vmware/Virtualbox

Cấu hình mạng trong phần mềm mô phỏng VMware đóng vai trò quan trọng trong việc kết nối các máy ảo (VM) với nhau hoặc với internet. Dưới đây là các chế độ mạng phổ biến và cách hoạt động của chúng trong cả hai phần mềm:

1.2.1 Các chế độ mạng trong VMware & VirtualBox

1.2.1.1 Bridged (Cầu nối)

- Máy ảo kết nối trực tiếp với mạng vật lý như một máy tính thực.
- Máy ảo nhận IP từ DHCP của router/mạng LAN.
- Có thể giao tiếp với các thiết bị khác trong cùng mạng LAN.
- Dùng khi muốn máy ảo hoạt động như một máy tính thực trong mạng.
- Ứng dụng: Máy chủ web, máy chủ cơ sở dữ liệu, ứng dụng cần kết nối thực.

1.2.1.2 NAT (Network Address Translation)

- Máy ảo dùng IP riêng và truy cập internet thông qua IP của máy chủ (host).
- Máy ảo không thể nhận kết nối từ bên ngoài.
- Dễ dàng thiết lập mà không cần cấu hình mạng.
- Ứng dụng: Dùng để lướt web, cài đặt phần mềm, kiểm tra ứng dụng mà không cần mở port.

1.2.1.3 Host-Only (Chỉ máy chủ)

- Tạo mạng riêng giữa máy chủ (host) và máy ảo (VM), không có internet.
- Dùng cho việc kết nối máy ảo với nhau mà không ảnh hưởng đến mạng bên ngoài.
- Ứng dụng: Mô phỏng môi trường mạng nội bộ, kiểm tra bảo mật.

1.2.1.4 Internal (Mạng nội bộ)

- Các máy ảo có thể giao tiếp với nhau nhưng không kết nối với máy chủ (host) hoặc internet.
- Chỉ sử dụng được giữa các máy ảo trong cùng một máy chủ ảo hóa.
- Ứng dụng: Mô phỏng hệ thống mạng riêng biệt mà không ảnh hưởng đến bên ngoài.

1.2.1.5 Custom Network (Mạng tùy chỉnh)

- Trong VMware, có thể tạo các mạng ảo riêng (VMnet0, VMnet1, VMnet8,...) với từng chế độ khác nhau.
- Cho phép mô phỏng môi trường phức tạp hơn với nhiều máy ảo và mạng con.
- Ứng dụng: Mô phỏng hạ tầng mạng lớn với nhiều tầng truy cập.

1.2.2 So sánh VMware và VirtualBox

Tính năng	**VMware**	**VirtualBox**
Giao diện	Dễ sử dụng	Đơn giản, miễn phí
Hiệu suất	Tốt hơn, tối ưu hóa tốt	Chậm hơn một chút
Hỗ trợ phần cứng	Rất tốt, tối ưu phần cứng	Hỗ trợ tốt nhưng không bằng Vmware
Cấu hình mạng	Linh hoạt, nhiều tùy chọn	Đầy đủ nhưng không chuyên sâu như VMware
Giá thành	Bản Workstation Pro có phí, Workstation Player miễn phí	Miễn phí hoàn toàn

1.2.3 Cách thiết lập mạng trong VMware và VirtualBox

1.2.3.1 VMware Workstation

- Vào Edit → Virtual Network Editor để cấu hình mạng.
- Chọn VM cần chỉnh → Settings → Network Adapter.
- Chọn chế độ Bridged, NAT, Host-Only hoặc tùy chỉnh.

1.2.3.2 VirtualBox

- Chọn máy ảo → Settings → Network.
- Chọn Adapter 1, Adapter 2,... và đặt chế độ NAT, Bridged, Host-Only,....
- Nếu cần mạng tùy chỉnh, vào File → Host Network Manager để tạo mạng riêng.

1.2.4 Khi nào nên chọn chế độ mạng nào?

Mục đích sử dụng	**Chế độ mạng khuyến nghị**
Duyệt Web, cài phần mềm	NAT
Kết nối vào mạng LAN như áy thật	Bridged
Kết nối giữa máy ảo và host, không ra internet	Host-only
Kết nối giữa các máy ảo, không kết nối host	Internal
Mô phỏng hệ thống mạng lớn	Custom (Vmnet – Vmware)

CHƯƠNG 2. NỘI DUNG THỰC HÀNH

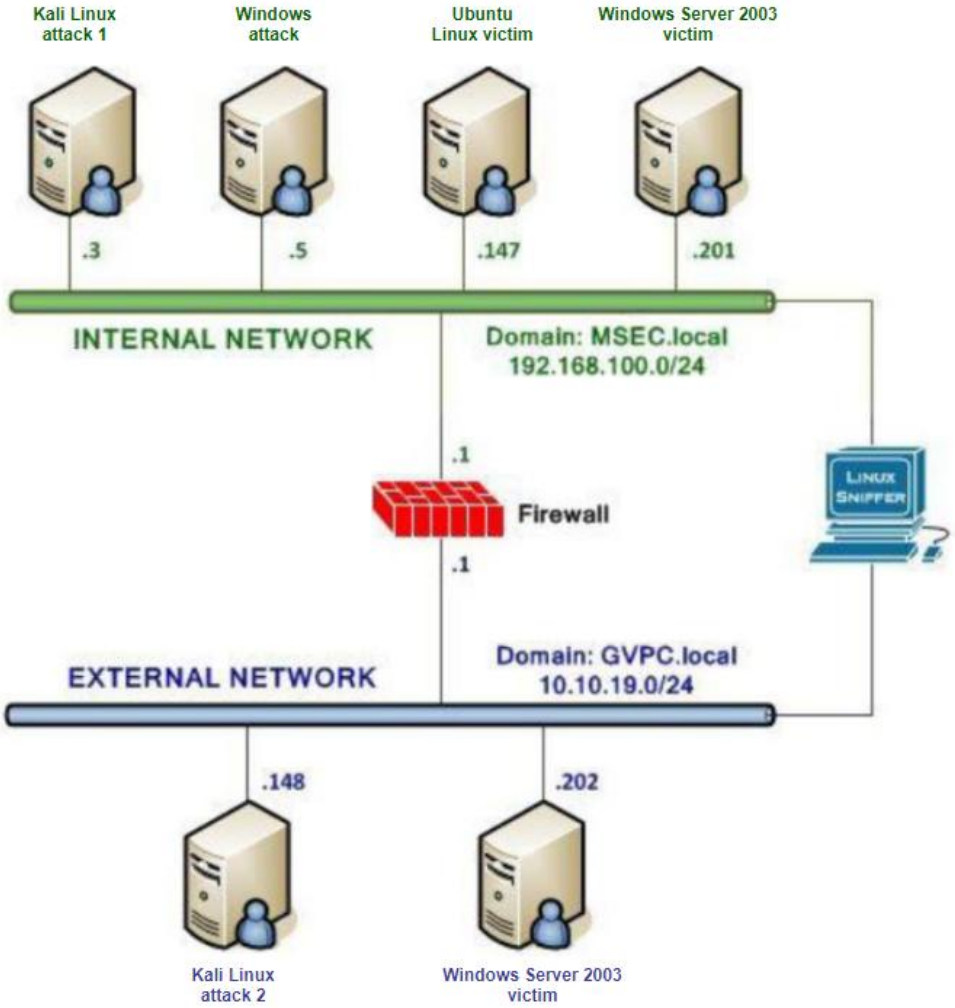
2.1 Chuẩn bị môi trường

- Phần mềm VMWare Workstation.
- Các file máy ảo VMware đã cài đặt trong các bài lab trước đó: máy trạm, máy chủ Windows 2019 và Linux.
- File cài đặt tường lửa Pfsense

2.2 Các bước thực hiện

2.2.1 Cấu hình topo mạng

Cài đặt và cấu hình hệ thống theo topo mạng và thông tin như mô tả dưới đây (bao gồm cài đặt các máy ảo)



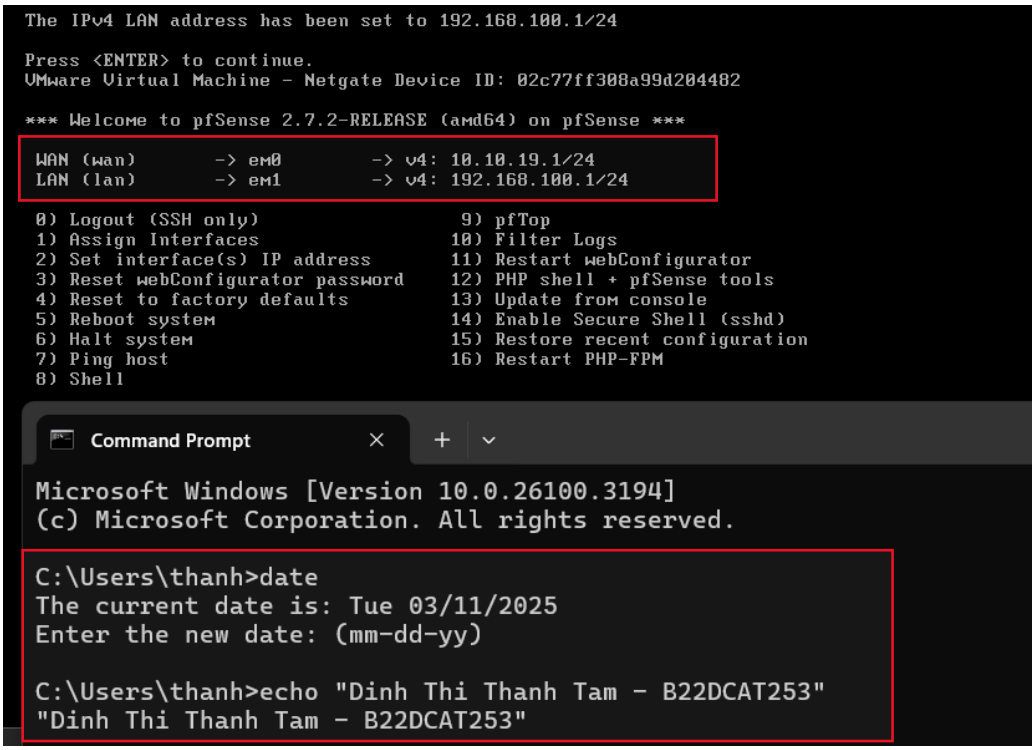
Thông tin yêu cầu cho các thiết bị trong hệ thống:

▪ Máy Kali Linux attack 1 trong mạng Internal	▪ IP: 192.168.100.3 ▪ Mật khẩu root: password
▪ Máy Windows Server 2003 Victim trong mạng Internal	▪ IP: 192.168.100.201 ▪ Mật khẩu root: password
▪ Máy Linux Victim trong mạng Internal	▪ IP: 192.168.100.147 ▪ Mật khẩu root: password
▪ Máy pfSense Firewall	▪ IP: 10.10.19.1, 192.168.100.1 ▪ Mật khẩu: admin/pfsense
▪ Máy Linux Attack trong mạng External	▪ IP: 10.10.19.148 ▪ Mật khẩu root: password
▪ Máy Windows Server 2003 Victim trong mạng External	▪ IP: 10.10.19.202 ▪ Mật khẩu root: password

Tiến hành ping thử các máy trong mạng

2.2.2 Cài đặt cấu hình pfsense firewall cho lưu lượng ICMP

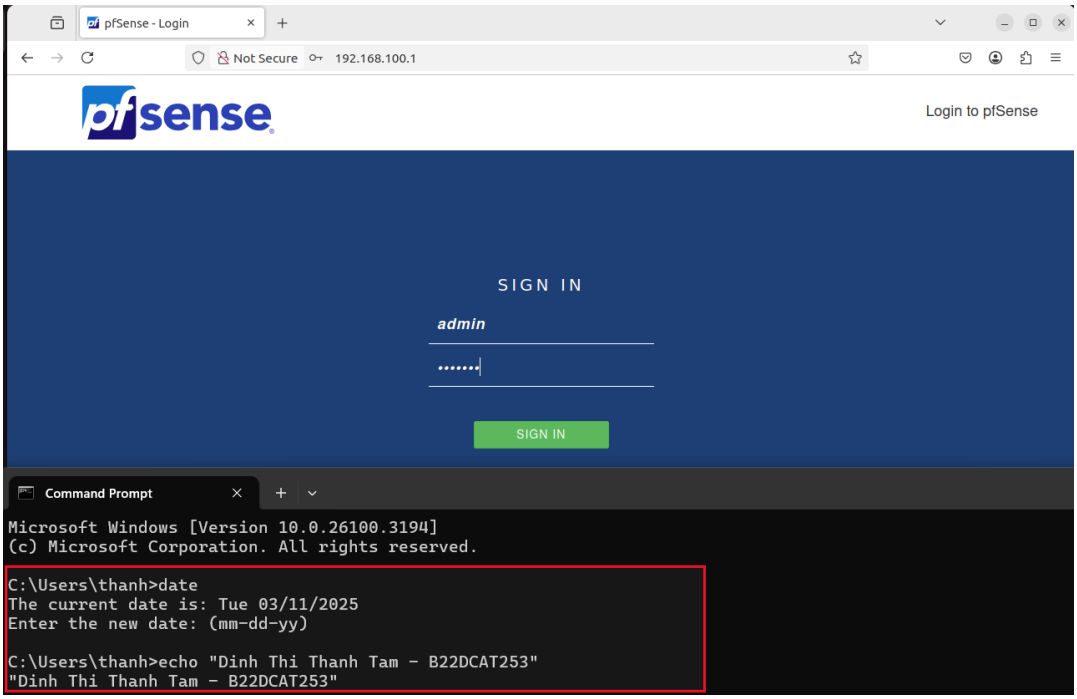
- Cấu hình máy pfSense Firewall IP: 10.10.19.1, 192.168.100.1



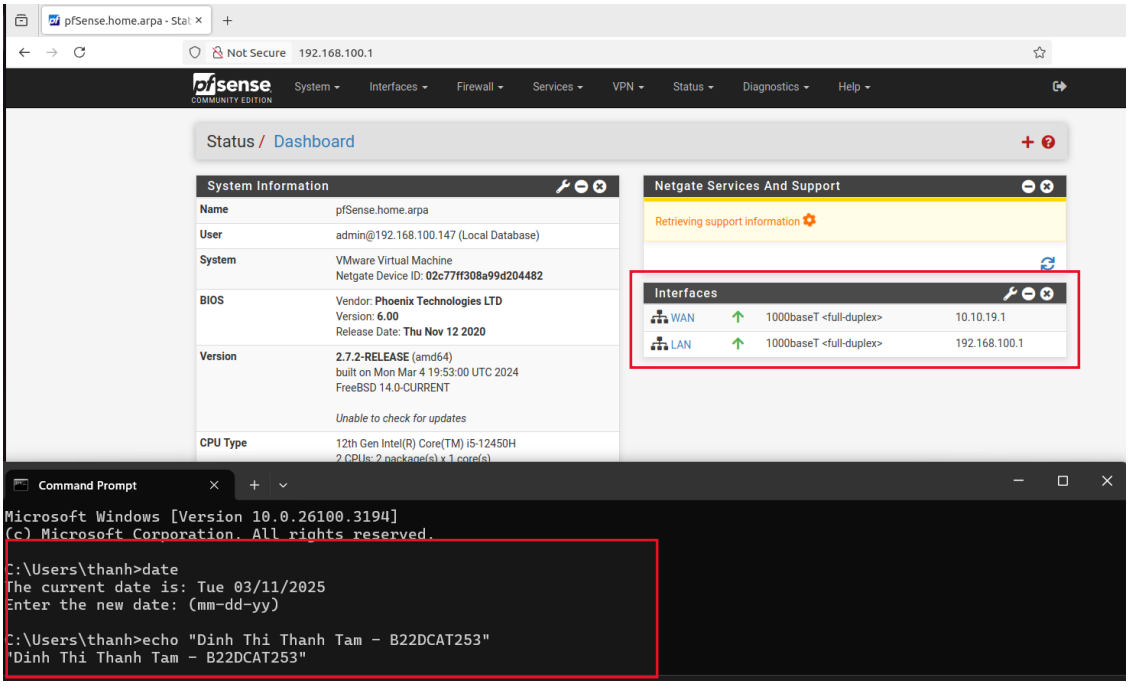
- Cấu hình ICMP cho phép các máy trong mạng Internal ping được ra các máy ở mạng External, không cho phép ping vào trong mạng Internal. Các bước lần lượt như sau:

2.2.2.1 Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình pfsense qua giao diện web

- Trên máy Linux Victim (Internal), mở trình duyệt và truy cập: http://192.168.100.1.
- Đăng nhập với tài khoản: admin/pfsense.



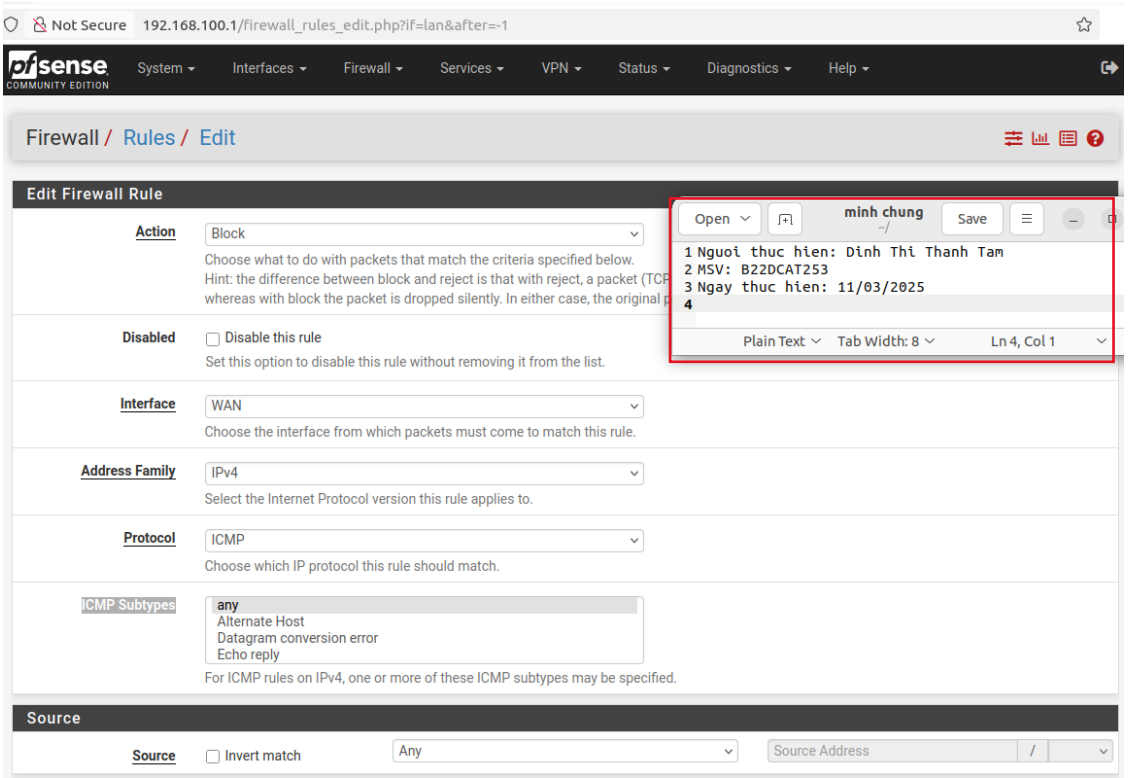
- Cấu hình firewall cho phép ICMP từ Internal ra External nhưng chặn ICMP từ External vào Internal.
- Yêu cầu
    - Cho phép gói tin ICMP (ping) từ mạng LAN (Internal) ra WAN (External).
    - Chặn gói tin ICMP từ mạng WAN (External) vào LAN (Internal).



2.2.2.2 Cấu hình Firewall pfSense để cho phép ICMP từ Internal ra External và chặn ICMP từ External vào Internal

Thêm quy tắc Firewall

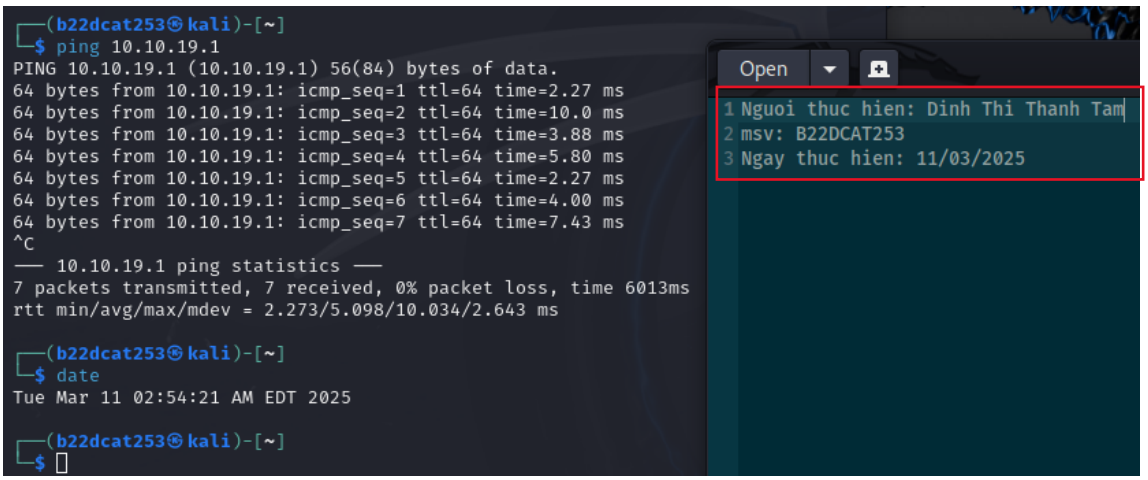
- Vào Firewall → Rules → Chọn tab WAN
- Nhấn Add để tạo quy tắc mới
- Cấu hình như sau:
    - Action: Pass
    - Interface: WAN
    - Address Family: IPv4 hoặc IPv4+IPv6
    - Protocol: ICMP
    - Source: any
    - Destination: any (hoặc WAN net nếu muốn giới hạn)
    - Description: Allow ICMP from LAN to External
    - Nhấn Save => Apply Changes



2.2.2.3 Kiểm tra bằng cách ping tới 10.10.19.1 từ máy Kali attack ở mạng ngoài.

- Dùng lệnh:

  Ping 10.10.19.1



⇨ Ta thấy luồng ICMP ở mạng External ping được tới giao diện 10.10.19.1

- Trả lời câu hỏi: Theo mặc định, có bao nhiêu cổng TCP mở trên giao diện mạng trong của pfSense?

Các cổng TCP mở mặc định trên pfSense

Cổng	**Dịch vụ**	**Mô tả**
80 hoặc 433	WebGUI (HTTP/HTTPS)	Giao diện quản lí webcuar pfSense. Mặc định dùng HTTPS(443)
22	SSH (nếu bật)	Dùng để truy cập psSense qua SSH. Mặc định bị tắt
53	DNS Resolver/Forwarder	Dịch vụ DNS nếu được kích hoạt
500	IPSec VPN	Dùng để thiết lập VPN Ipsec
1194	OpenVPN	Nếu có cấu hình OpenVPN
1812	RADIUS (nếu bật)	Dịch vụ xác thực người dùng

⇨ Lưu ý:

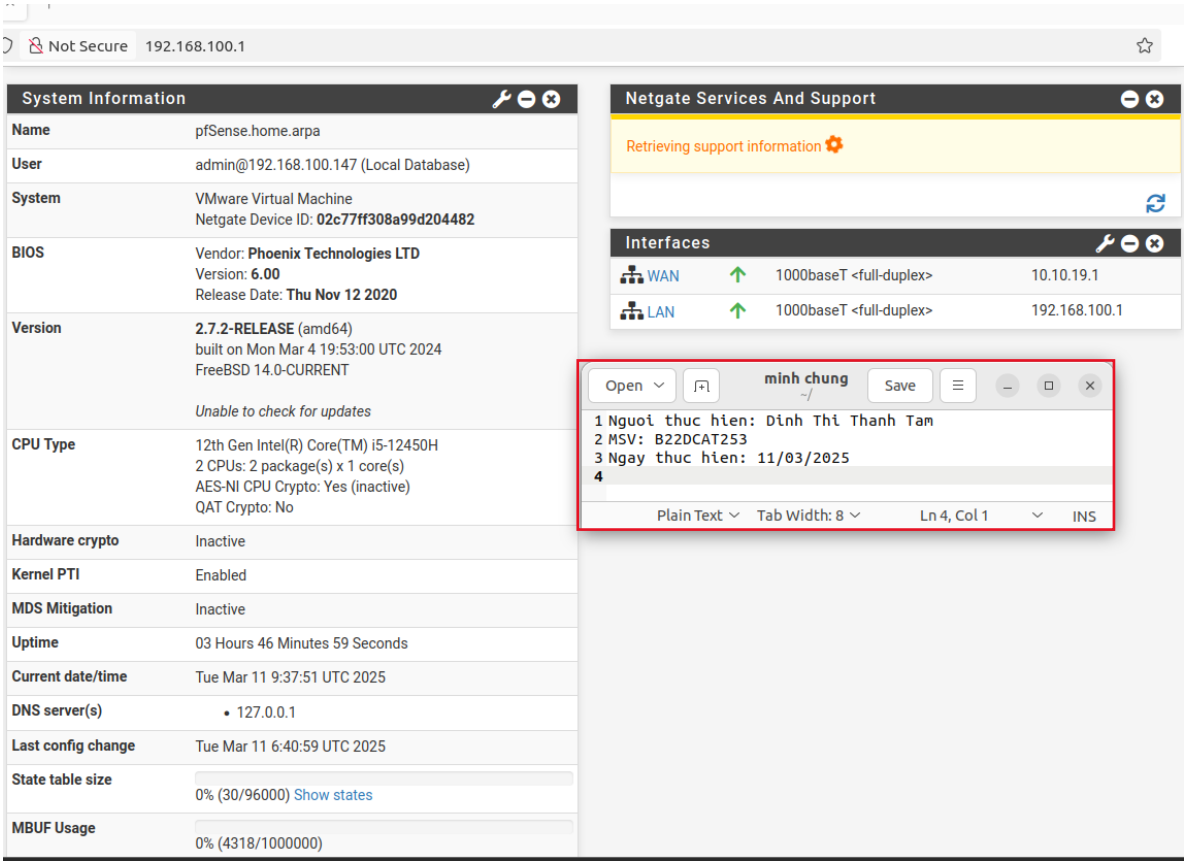
- pfSense không mở cổng trên WAN trừ khi người dùng cấu hình firewall rules cho phép.
- Có thể kiểm tra cổng mở bằng lệnh *netstat -an* trên pfSense hoặc dùng nmap từ máy khác để quét.

2.2.3 Cài đặt cấu hình pfsense firewall cho phép chuyển hướng lưu lượng tới các máy trong mạng Internal

Cấu hình tường lửa cho phép 1 cổng và chuyển hướng lưu lượng:

2.2.3.1 Truy cập pfsense qua giao diện web

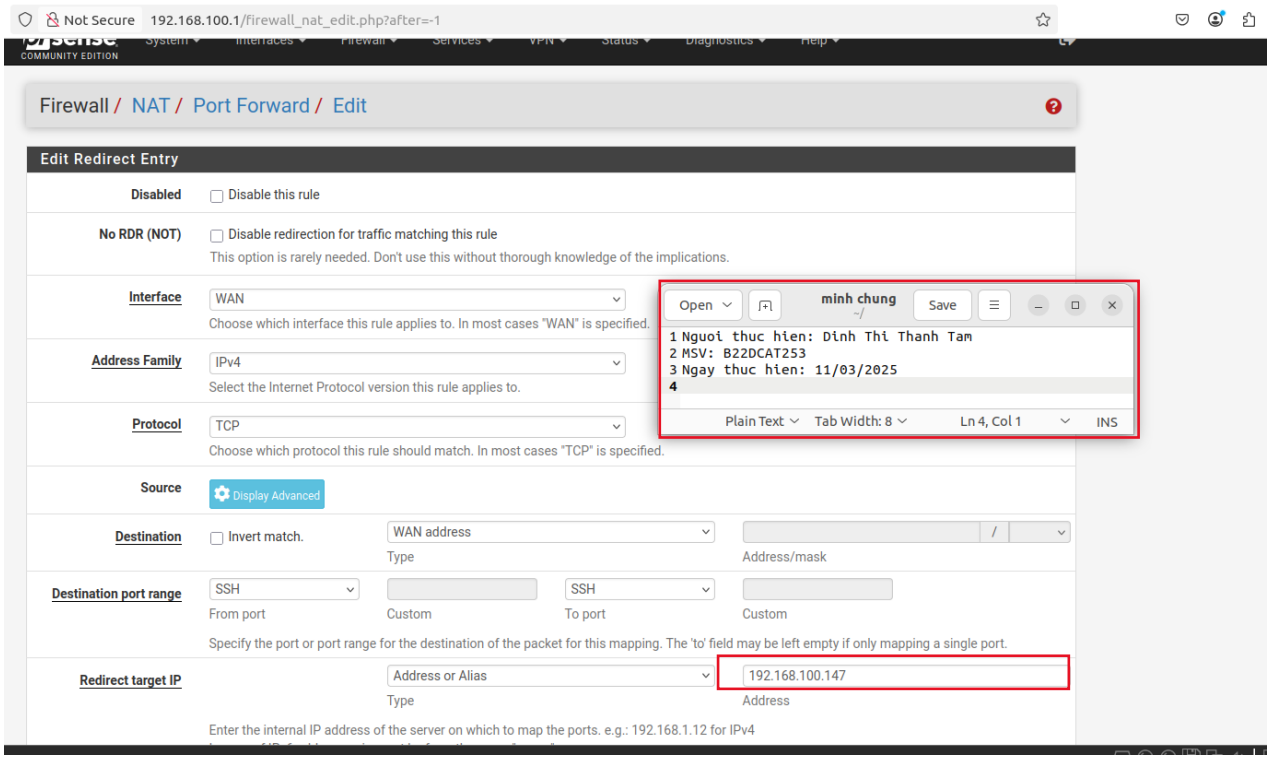
Trên máy Linux victim ở mạng trong, vào http://192.168.100.1 để cấu hình NAT trên pfsense qua giao diện web.



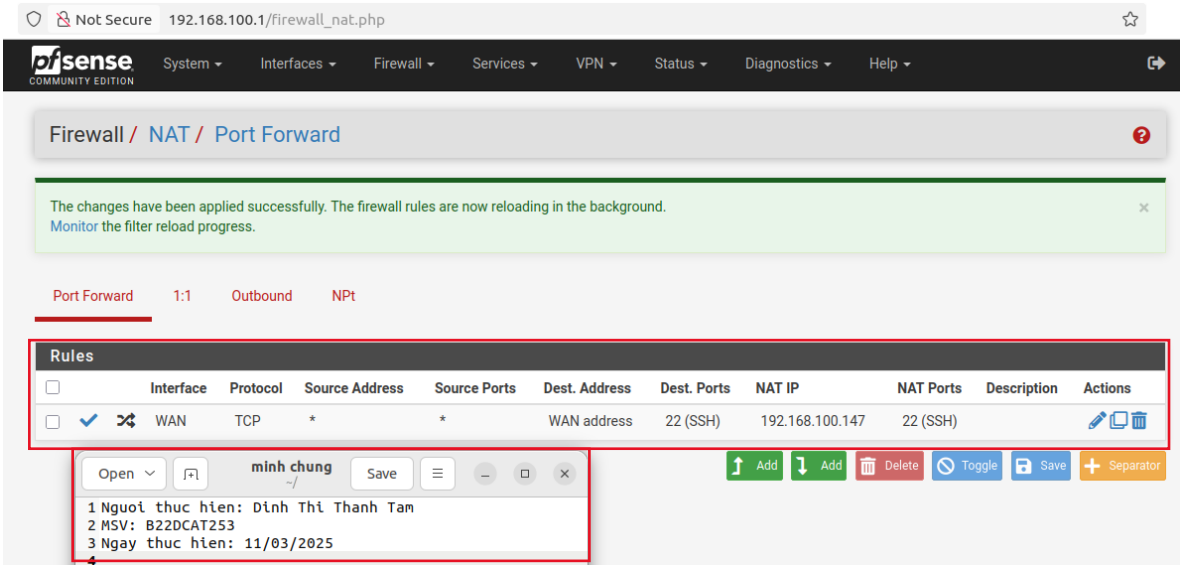
2.2.3.2 Cấu hình NAT để chuyển hướng cổng SSH

Khi có kết nối SSH từ mạng External (10.10.19.0/24) vào IP của Pfsense (10.10.19.1), nó sẽ chuyển tiếp đến máy Linux Victim (192.168.100.147).

- Trong giao diện pfSense, vào Firewall -> NAT -> Port Forward.
- Nhấn Add để tạo quy tắc mới và điền thông tin như sau:
    - Interface: WAN (hoặc giao diện nhận kết nối từ ngoài, ở đây là 10.10.19.1)
    - Protocol: TCP
    - Destination: WAN Address
    - Destination Port Range: SSH
    - Redirect Target IP: 192.168.100.147
    - Redirect Target Port: SSH
    - Nhấn Save và Apply Changes.



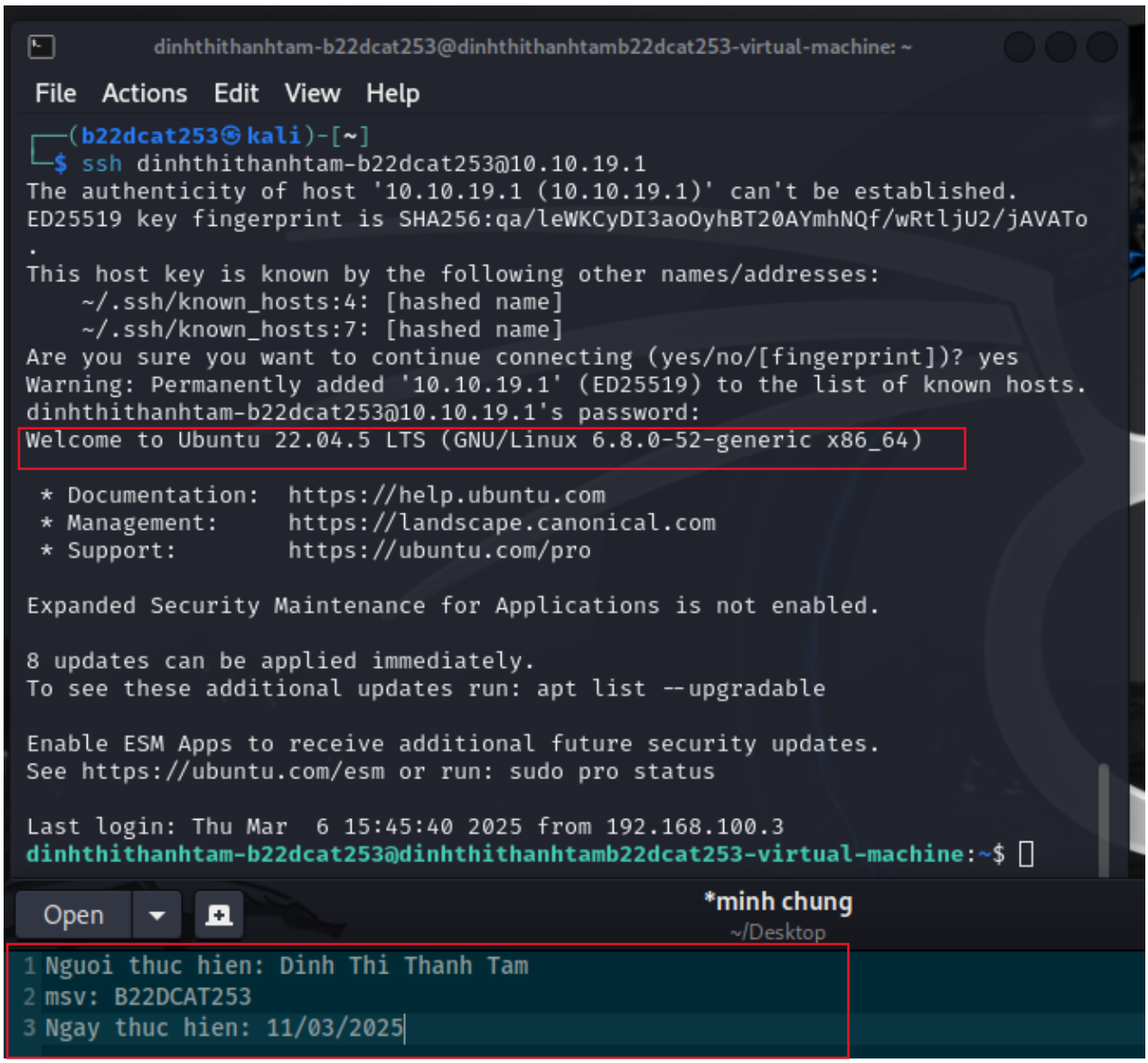
Sau khi hoàn thành, luật mới tạo đã được thêm



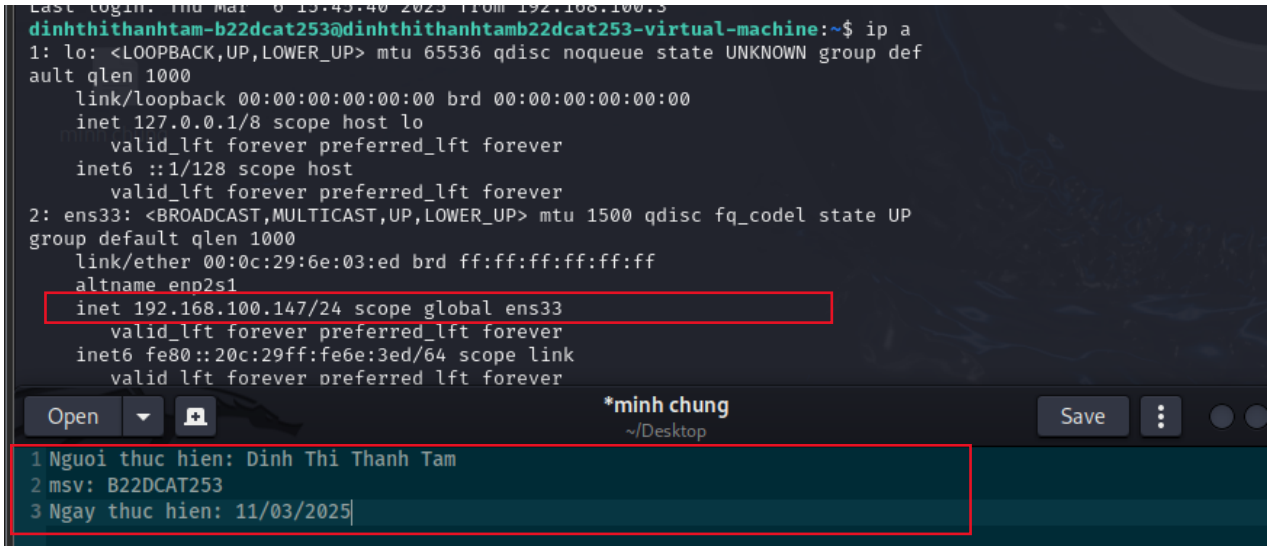
2.2.3.3 Kiểm tra kết nối

- Kiểm tra bằng cách truy cập ssh tới 10.10.19.1 từ máyLinux có IP 10.10.19.148 bằng lệnh:

  ssh dinhthithanhtam-b22dcat253@10.10.19.1



- Sau đó gõ ifconfig để kiểm tra IP máy có phải là 192.168.100.147 hay không?



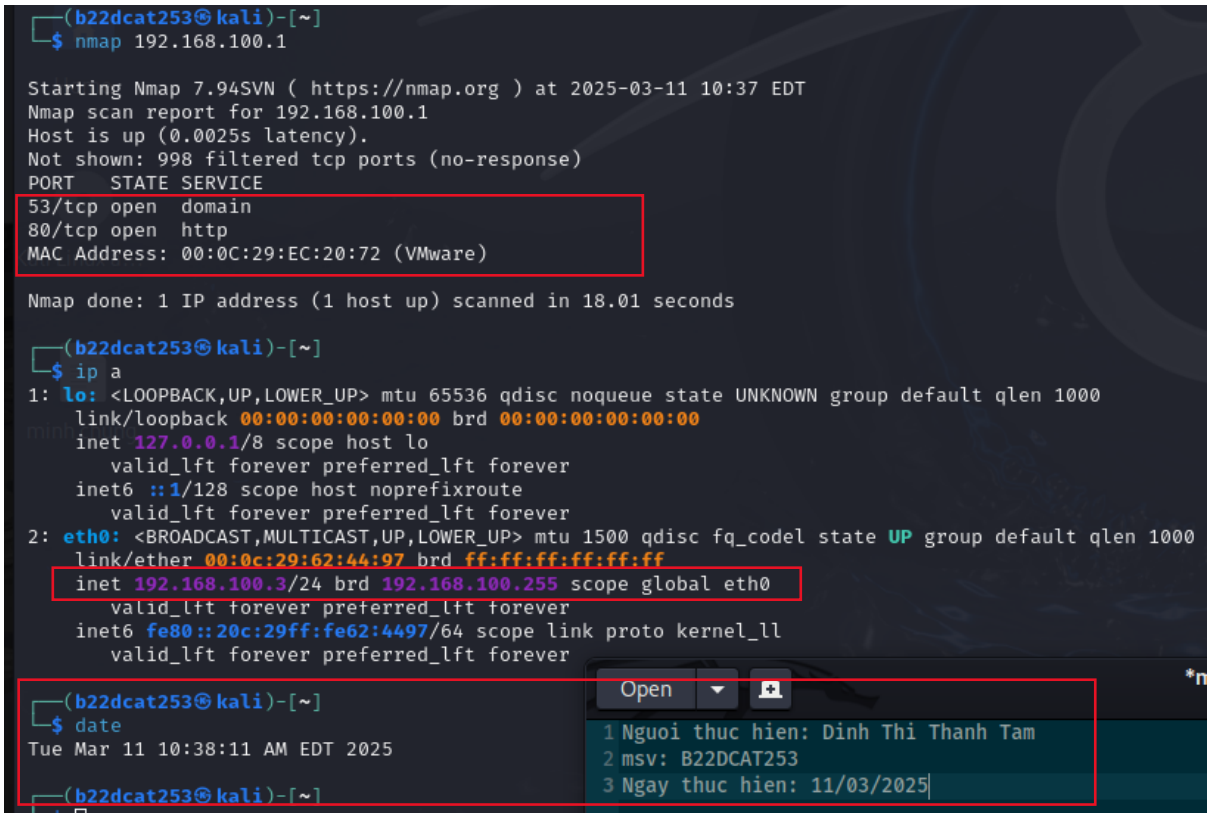
➔ Kết nối SSH từ bên ngoài (mạng 10.10.19.0/24) đến máy Linux victim (192.168.100.147) qua pfSense thành công, điều đó có nghĩa là:

- NAT (Port Forwarding) hoạt động đúng: pfSense đã chuyển tiếp kết nối SSH từ WAN (10.10.19.1) đến máy Linux victim trong mạng LAN (192.168.100.147).
- Firewall Rules đúng: Quy tắc firewall trên pfSense đã cho phép lưu lượng SSH từ bên ngoài đi qua.
- Dịch vụ SSH trên máy Linux đang chạy: Máy Linux victim đang lắng nghe trên cổng SSH (22) và chấp nhận kết nối từ bên ngoài.
- pfSense không chặn kết nối: Không có quy tắc nào trên firewall chặn lưu lượng SSH.

2.2.3.4 Kiểm tra các cổng được phép truy cập trên mạng Internal

Trên máy Kali Linux trong mạng Internal, gõ lệnh:

nmap 192.168.100.1



➔ Kết quả quét cổng bằng Nmap (nmap 192.168.100.1)

- Hai cổng TCP đang mở:
    - 53/tcp (DNS)
    - 80/tcp (HTTP - có thể là giao diện web của pfSense).
    - Các cổng khác bị lọc (filtered), nghĩa là firewall có thể đang chặn.

KẾT LUẬN

Bài thực hành giúp sinh viên hiểu rõ hơn về cách thiết lập và quản lý một hệ thống tường lửa trong môi trường doanh nghiệp. Thông qua việc cài đặt và cấu hình PfSense, sinh viên đã có cơ hội thực hành các kỹ thuật bảo mật quan trọng, bao gồm quản lý luồng truy cập mạng, thiết lập NAT và kiểm soát truy cập bằng firewall.

Quá trình thực hiện cho thấy việc bảo mật hệ thống mạng không chỉ đơn thuần là cài đặt phần mềm mà còn đòi hỏi kiến thức về quản lý hệ thống, phân tích và đánh giá rủi ro. Bài thực hành cũng giúp sinh viên nâng cao kỹ năng làm việc với máy ảo, cấu hình mạng trên VMware và sử dụng các công cụ kiểm tra an ninh mạng như nmap, SSH.

TÀI LIỆU THAM KHẢO

[1] Lab 7 pfsense firewall của CSSIA CompTIA Security+®

[2] Advanced Penetration Testing for Highly-Secured Environments Second Edition

[3] Giới thiệu về Pfsense: https://viblo.asia/p/network-gioi-thieu-ve-pfsense-N0bDM6LXv2X4